Bitcoin

- Bitcoin is a completely decentralized, peer-to-peer, permissionless cryptocurrency.

Completely decentralized: no central party for ordering or recording anything.

Peer-to-Peer :- S/w that runs on machines of all stakeholders to form the system.

Permissionless :- no identity, no need to signup anywhere to use ; no access control - anyone can participate in any role.

→ Bitcoin mining components:

① Nodes ② Mining pools
③ Miners ④ Large Miners

→ The technology behind the Bitcoin - the Blockchain

→ The Bitcoin Transaction Life Cycle - The Sender

Alice opens her bitcoin Wallet → Provides the address of Bob and the amount to transfer, and send.

~~Life cycle~~ - The Network

The wallet constructs the transactions, sign using Alice's private key and broadcasts it to the network. ⟹ The network nodes validate the transactions based on the existing blockchain and propagate the transaction to the miners. ⟹ The miners include the transaction to the next block to be mined.

Life cycle - The Miners :

The miners collect all the transactions for the a time duration, say for 10 Minutes

⟹

Miners construct a new block and tries to connect it with the existing blockchain, through a cryptographic hash computation.

The Mining Procedure

⟹

Once the mining is over and the hash is obtained, the block is included in the existing blockchain. The updated blockchain is propagated in the network.

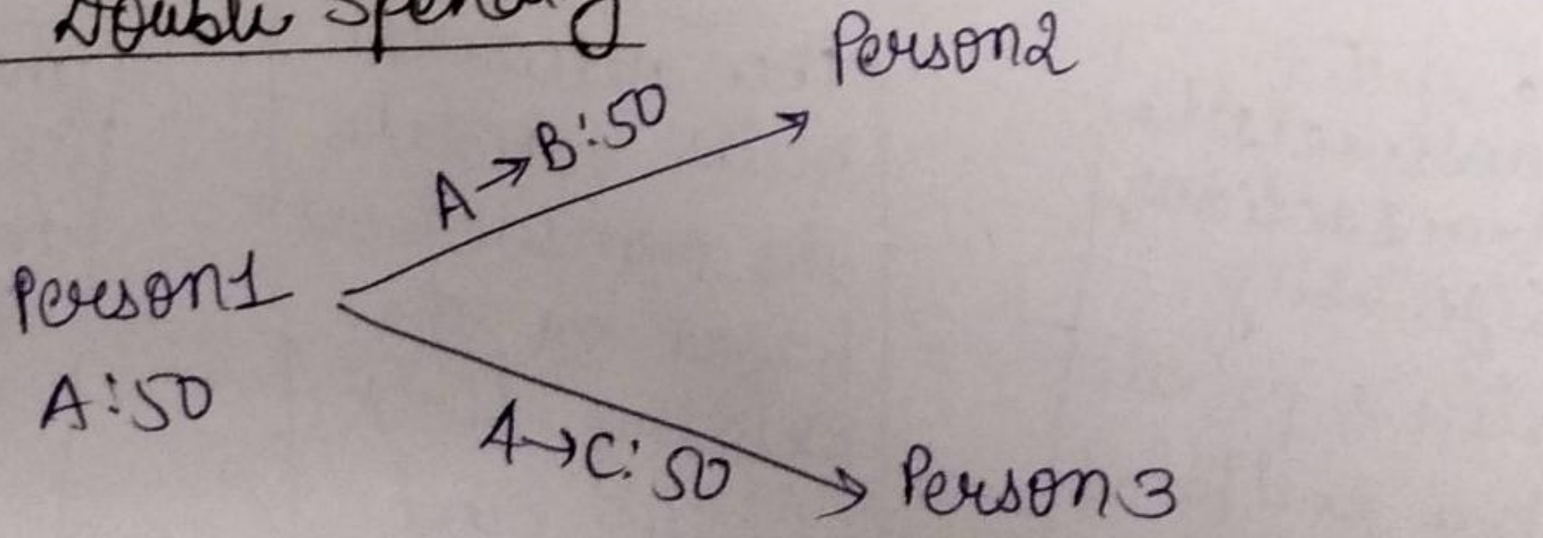
Life cycle - the Receiver:

Bob opens his bitcoin wallet and refreshes, the blockchain gets updated.

⟹

The transaction reflects at Bob's Wallet.

Bitcoin Double spending



Double-spending is the risk that a cryptocurrency can be used twice or more.
Transaction info. within a blockchain can be altered if specific conditions are met.

- Double-spending occures when something someone alters a blockchain network and inserts a special one that allows them to reacquire a cy cryptocurreng.

→ Bitcoin block Propagation whenever a node is getting more than one copy of the blockchain, it will accept the copy which has been transferred by maximum no. of peers.

→ Block Header (Bitcoin)

Fig:- Contents of a block header.

Split up details	Block Header Contents (80 byte)
4 Byte	Bitcoin version number
32 Byte	Previous block hash
32 Byte	Merkle Root
4 Byte	Time stamp
4 Byte	Difficulty Target
4 Byte	Nonce used by miners.
80 bytes	Total

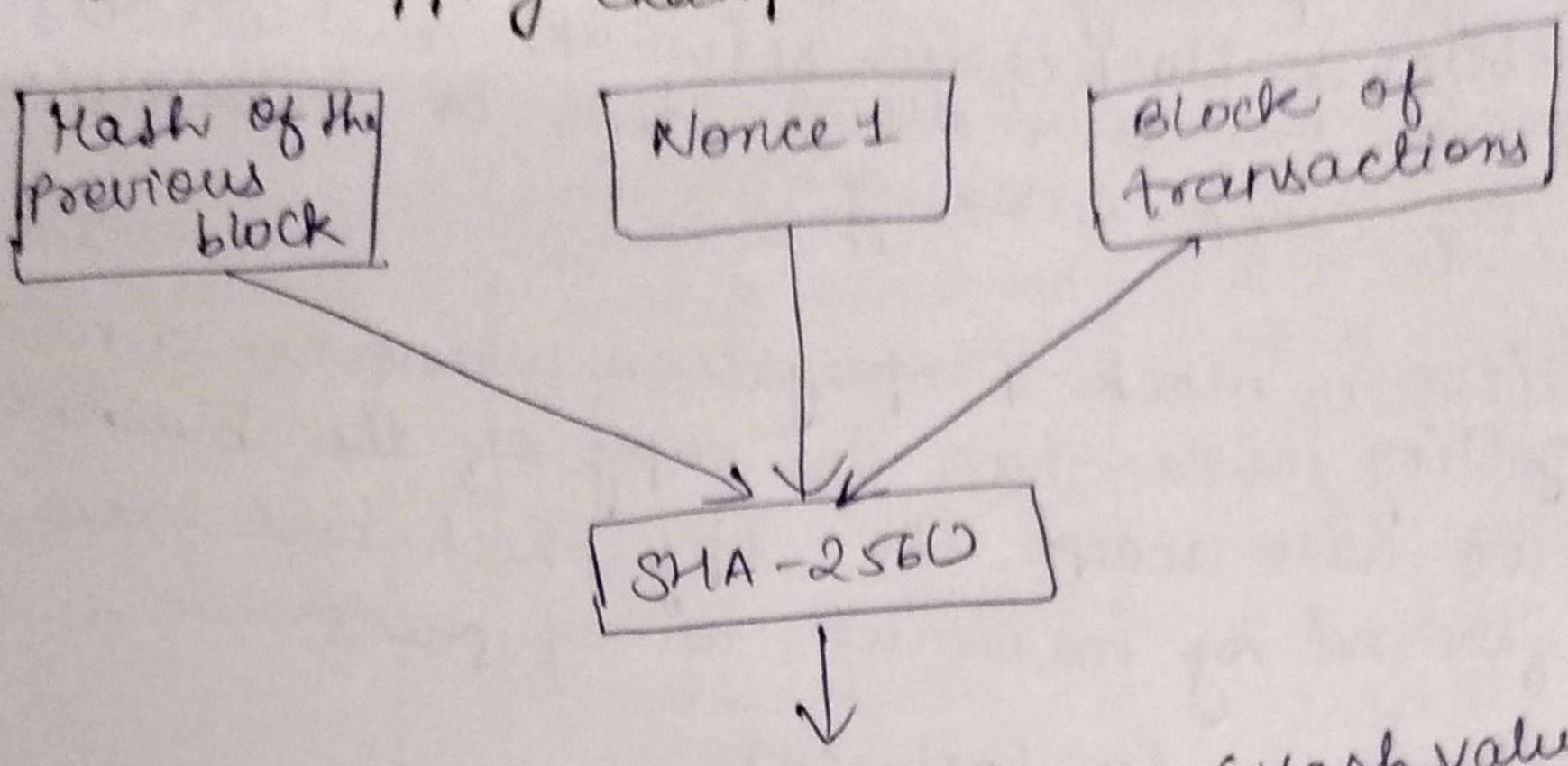
→ Block identifier – the hash of the current block header (Hash algo: Double SHA 256).

→ Previous block hash is used to compute the current ~~to~~ block hash.

→ Transactions in a Block (Bitcoin):

- Transactions are Organized as a Merkel Tree. The Merkle Root is used to construct the block hash.
- If you change a transaction, you need to change all the subsequent block hash.

→ Hashcash mapping example 1.



(Hash value)

00005 57c - ——

→

	Bitcoin	Visa	MasterCard
Transactions per second	7	65,000	40,000
Total no. of transaction in year 2018	81 Million	124 billion	74 Billion

→ What is cryptocurrency?

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it ~~mea~~ nearly impossible to counterfeit or double spend.

→ The advantages of cryptocurrencies include cheaper and faster money transfers and decentralized systems that do not collapse at a single point of failure.

→ The disadvantages of cryptocurrencies include their price volatility, high energy consumption for mining activities, ~~a~~ and use in criminal activities.

Merkle Tree

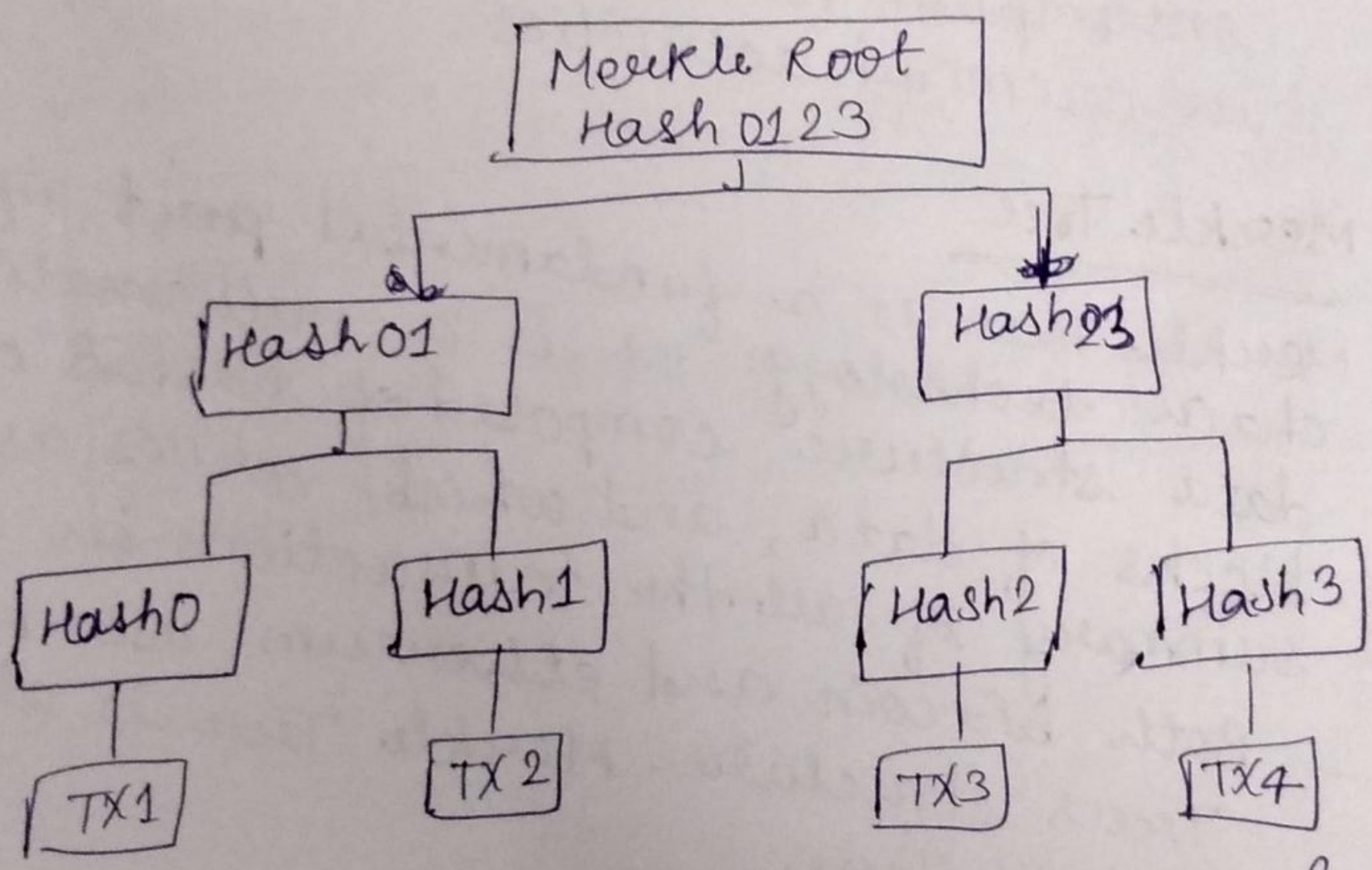
Merkle Tree is a fundamental part of blockchain technology. It is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block.

→ Both bitcoin and ethereum use Merkle Trees structure. Merkle Tree is also known as Hash Tree.

→ A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not.

→ Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle root or root hash. The Merkle trees are constructed in a bottom-up approach

→ Merkle trees are in a binary tree, so it requires an even number of leaf nodes. If there is an odd number of transactions, the ~~be~~ last hash will be duplicated once to create an even number of leaf nodes.



→ Merkle root is stored in the block header.

→ Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA)
- Based on elliptic curve cryptography
- Supports good randomness in key generation.

Types of Blockchains :-

1. Public Blockchain
2. Private Blockchain
3. Consortium "
4. Hybrid "

Crypto Currency

It is a digital currency in which cryptography techniques are used to regulate the generation of units of currency and verify the transfer funds.

— Transactions are irreversible.

→ Crypto currency Vs conventional currency :-

Type	Conventional currency	Cryptocurrency
	Real	Virtual
Intermediate	Yes	No (Peer to peer)
Portability	Yes (except too much cash)	Highly portable
Durable	Moderate	Highly durable
Acceptance	National	Global
Secure	Moderate	High
Scarce	Low	High
Decentralized	No	Yes
Smart	No	Yes

Why we use crypto currency?

- Fast and cheap
- Easy to use
- Free to transfer and hold
- Decentralized control
- Privacy and security
- Transparency is maintained through public ledger system.
- Reduced Fraud

** Forcking :- Duplication from existing blockchain

- A fork is a change to the digital currency S/W which creates two different paths of the blockchain with a shared history.
- The forks can be temporary, or lasting for a few minutes, or can be permanent.

① Soft Fork

- A soft fork introduces a change which is backwards compatible with the previous version. It means there is no need to upgrade the older version of the bitcoin S/W necessarily.

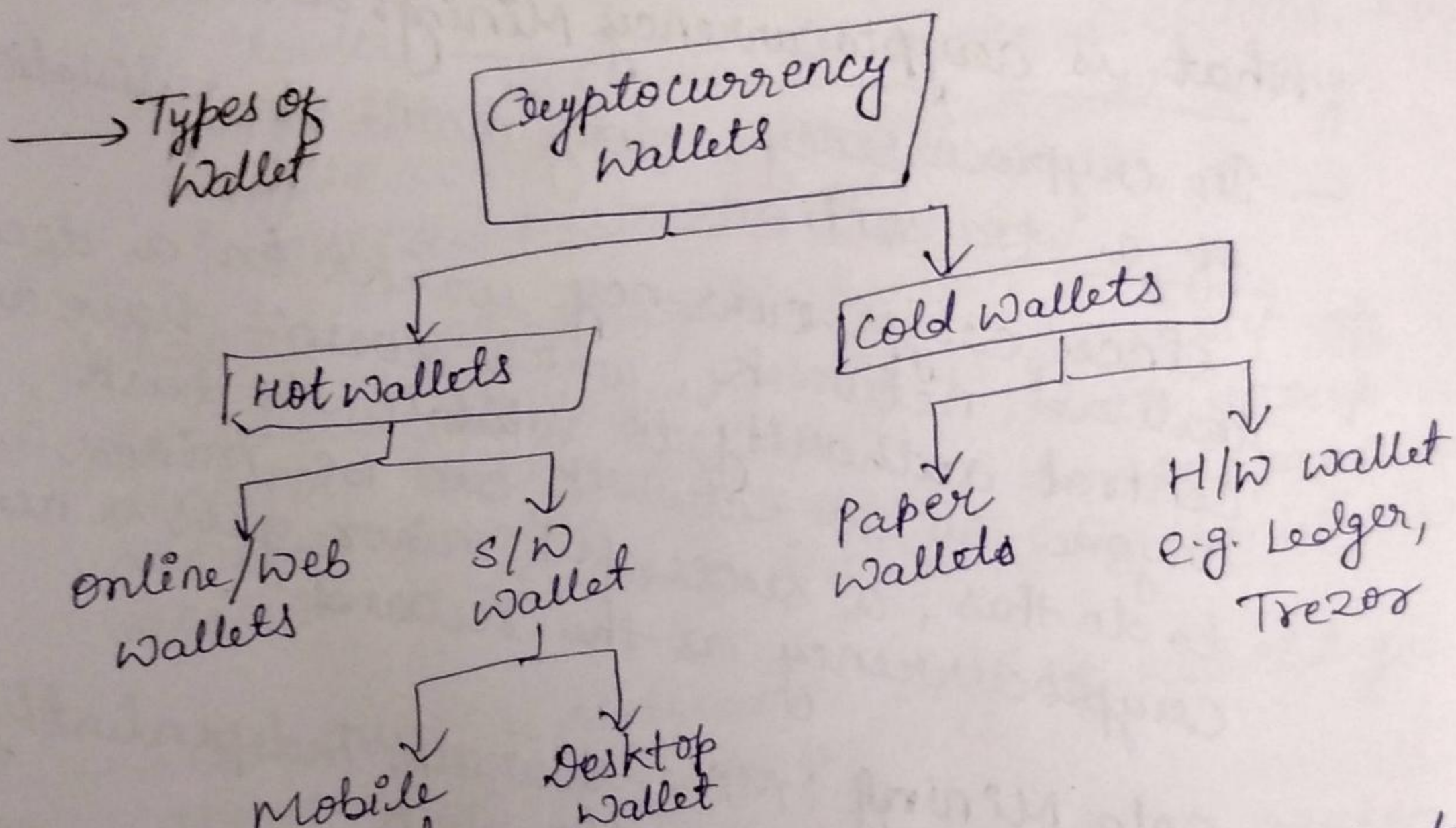
→ It is called soft because both groups of users (old and new users) will continue to mine new blocks on the same blockchain.

② Hard Fork:

- A hard ford introduces a change that forces everyone to upgrade the S/W. The hard fork is not backwards compatible with older versions of the S/W.

e.g. Bitcoin Cash Fork

→ Types of Wallet



Cryptocurrency Wallet :- S/W program that stores the user's public and private keys enabling the user to transmit Crypto assets.

Hot Wallet : Online day to day transactions. It is connected to Internet.
Desktop Wallet, Mobile Wallet, Online Wallet

Cold Wallet : It is not connected to the internet and it is not free. They are used it for long time storage.

Types of Cryptocurrency:-

- Bitcoin
- Bitcoin cash
- Litecoin
- Ethereum
- Ripple
- Stellar

What is cryptocurrency Mining? or Bitcoin mining

- In cryptocurrency, mining means the validation of a transaction.

- Since cryptocurrency works on a decentralized network, which doesn't have any central authority to validate the task, anyone in the network can be minor, and to do this, a successful minor gets a new cryptocurrency as the reward.

Solo Mining: Miners work independently to mine the block.

Pool Mining: Group of miners join collectively.

CPU mining: Miner utilises CPU to mine the cryptocurrency.

Cloud Mining:- Miner rents out cloud mining services to other miners for pre assigned period.

Rudiments of consensus algorithms

→ In normal centralized organisation
- All the decisions are taken by the leader or a board of decision makers.

→ This isn't possible in a decentralised system such as blockchain because a blockchain has no "leader".
↳ for the blockchain to make decisions, they need to come to a consensus ~~ed~~ using "consensus Mechanisms".

What are consensus Mechanism?

Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole.

→ Consensus is a dynamic way of reaching agreement in a group.

→ A consensus makes sure that an agreement is reached which could benefit the entire group as a whole.

what is a consensus Algorithm?

Consensus algorithms are a decision-making process for a group, where individuals of the group construct and support that decision that works best for the rest of them.

→ Consensus algorithms do not merely agree with the majority votes, but it also agrees to one that benefits all of them.

Objectives of the Consensus Process:

(i) Coming to an agreement:
(ii) Collaboration
(iii) Co-operation
(iv) Equal Rights
(v) Participation
(vi) Activity

* The Byzantine Generals' Problem :-

Consider a group of generals, each commanding a portion of the Byzantine Army, encircle a city. They must decide whether to attack or retreat. But ~~whee~~ whatever they decide, the most important thing is that they reach a consensus. But consensus is difficult to reach, because generals don't know the decision of other generals.

consider the following :-

- There are 3 generals, general A, B and C.
- The generals must attack their enemy at the same time, otherwise they may risk failure.
- The generals have no effective way to communicate instantly.
- Therefore, they need to send a courier to others to transmit the message.
- The generals need to reach consensus before attacking.

— They must confirm that the other generals will attack at the same time.

— The problem complicates when we consider traitors may exist. We have no way to guarantee all of the messangers are trustworthy, and on top of that, a messanger could be captured and forced to deliver a forged messages.

→ Analogy b/w Byzantine Generals' Problem and blockchain Networks:—

From the Byzantine Generals' Problem, we can infer that:

— The generals in Byzantine represent nodes on a chain

— Each consensus formed by a group of generals represents a block.

— All the generals must confirm each other's decision to reach consensus before launching a coordinated attack. Similarly in a blockchain, all nodes must agree on the next block to be written.

→ Objectives of Consensus Protocol:—

A consensus mechanism is a fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement amongst members of the network on the transactions that are valid and can be updated on to the ledger.

Types of Consensus Algorithms :-

(i) Proof of Capacity (PoC) :-
using this protocol you can utilize the capacity or storage space of user's hard drive.

(ii) Proof of Burn (PoB) :-
Users send the coins back into their wallet that they can't recover from will get rewards based on the amount.

(iii) Proof of Weight (PoWeight)
Similar to PoS but the difference is that it depends on various other factors called weights.

(iv) Proof of Work :- (PoW):
When a user initiates a transaction, 'miners' or supercomputers try to solve a problem or puzzle to verify it.

(v) Proof of Stake (PoS):
A user is encouraged to spend more until he/she becomes a validator to create a block.

(vi) Delegated Proof of Stake (DPoS) :-
Same as PoS but users with more coins will get to vote and elect witnesses.

(vii) Leased Proof of Stake (LPoS):
Users will be able to make customize tokens and use it on their farms for better security.

(viii) Proof of Importance:-
User that frequently send and receive transactions will get paid ~~out~~ for that.

(ix) Proof of Activity (PoA):
Uses both PoS and PoW to ensure the reward points are on time.

(x) Directed Acyclic Graphs (DAGs):-
DAGs don't have blockchain data structure and can handle transactions asynchronously.

(xi) Delegated Byzantine Fault Tolerance (DBFT).
Focuses on a gamified way of a block verification among the professional node controllers.

(xii) Simplified Byzantine Fault Tolerance
A single Validator can bundle proposed transactions and create a new block

(xiii) Practical Byzantine Fault Tolerance (PBFT):-
Byzantine used a particular sequence to keep the rouge users at bay.

(xiv) Proof of Elapsed Time (PoET):-
Similar to PoW but the difference is that it focuses more on consumption.

* Proof Of Work (PoW) :—

Proof of work is the first blockchain algorithm introduced in the blockchain network. Many blockchain technologies uses this blockchain consensus models to confirms all of their transactions and produce relevant blocks to the network chain.

— The central principle behind this technology is to solve complex mathematical problems and easily give out solutions.

— The mathematical problems requires a lot of computational power, to begin with.

— However proof of work has certain limitations. The network seems to grow a lot, and with this, it needs lots of computational power. This process is ~~increas~~ increasing the overall sensitivity of the system.

key points :—

(i) The amount of work done by a particular miner determines his/her possibility of mining a single block and the reward of getting a coin.

(ii) The miners get lesser bitcoins over time Such smaller incentives ensure less chance of the 51 % attack.

(iii) The community-bond of the miners of PoW is extrelemely strong. Thus the possibility of the community to becomes more centralized increases with time.

Time critically

— Blockchain consensus sequence suites mostly on accurate data and information. However, the speed of the system lacks tremendously. If a problem becomes too complicated, it takes a lot of time to generate a block.

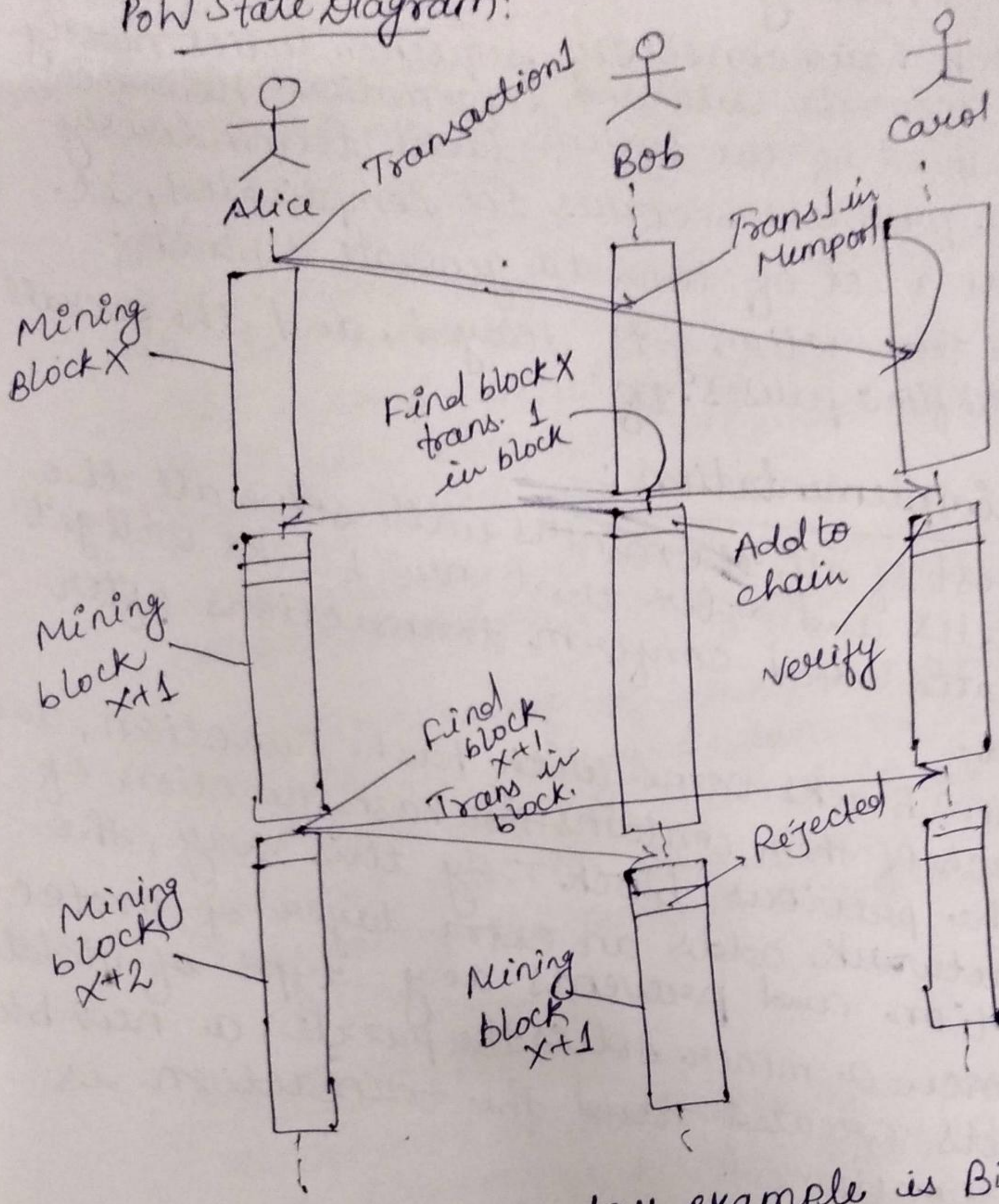
— The transaction gets delayed, and the overall workflow pauses.

→ PoW implementation :-

— First of all, the miners will solve all the puzzles and after that new blocks will get created and confirm transactions after that.

— New blocks come with hash Function, and each of them contains the hash function of the previous block. By this way, the network adds an extra layer of protection and prevents any type of violations. Once a miner solves the puzzle; a new block gets created, and the transaction is confirmed.

PoW State Diagram:



→ The most popular example is Bitcoin. Bitcoin introduced this type of consensus algorithm blockchain before any other crypto-currencies.

→ blockchain consessus models allowed any kind of change in the complexity of the puzzle, based on the overall power of the network.

- It takes about 10 minutes to create a new block.

→ Ethereum has moved on to Proof of Stake (PoS).

Issues of PoW

① Greater Energy consumption:

— Blockchain network contains millions and millions of designed microchip that hashes contantly.

— The greater consumption is becoming a problem in a world where we are running out of energy - miners on the system have to face a large sum of cost due to the electricity consumption.

② centralization of Miners:-

— With the energy problem, proof of work will move toward cheaper electricity solutions.

— This situation will lead towards centralization within the decentralized network. That's why it's another great problem these blockchain algorithms is facing.

③ The 51% Attack:

— This attack would mean a possible control of majority users and taking over most of the mining power. In this scenario, the attackers will get enough power to control everything in the network.

— They can stop other people from generating new blocks.

** Bitcoin Mining :-

Creation of bitcoin blocks is called mining.

→ Mining is the mechanism whereby nodes called "miners" in the Bitcoin world validate the new transactions and add them to the blockchain ledger.

Bitcoin mining components :

- Nodes
- Mining pools
- Miners
- Large Mines

doubt / another point

The probability that random hash value is within limit = $\frac{\text{Target Hash Set}}{\text{Population Hash Set}}$

$= 2 \times 10^{-22}$

Therefore, the chances of identifying the next value of the hash by changing the nonce are negligible.

→ A nonce is a finite no. with a 32-bit unsigned ~~numb~~ integer.

The maximum nonce $= 2^{32} = 4 \times 10^9$.

It has a value b/w zero and 4 billion (approximately).

Probability that one of them becomes valid

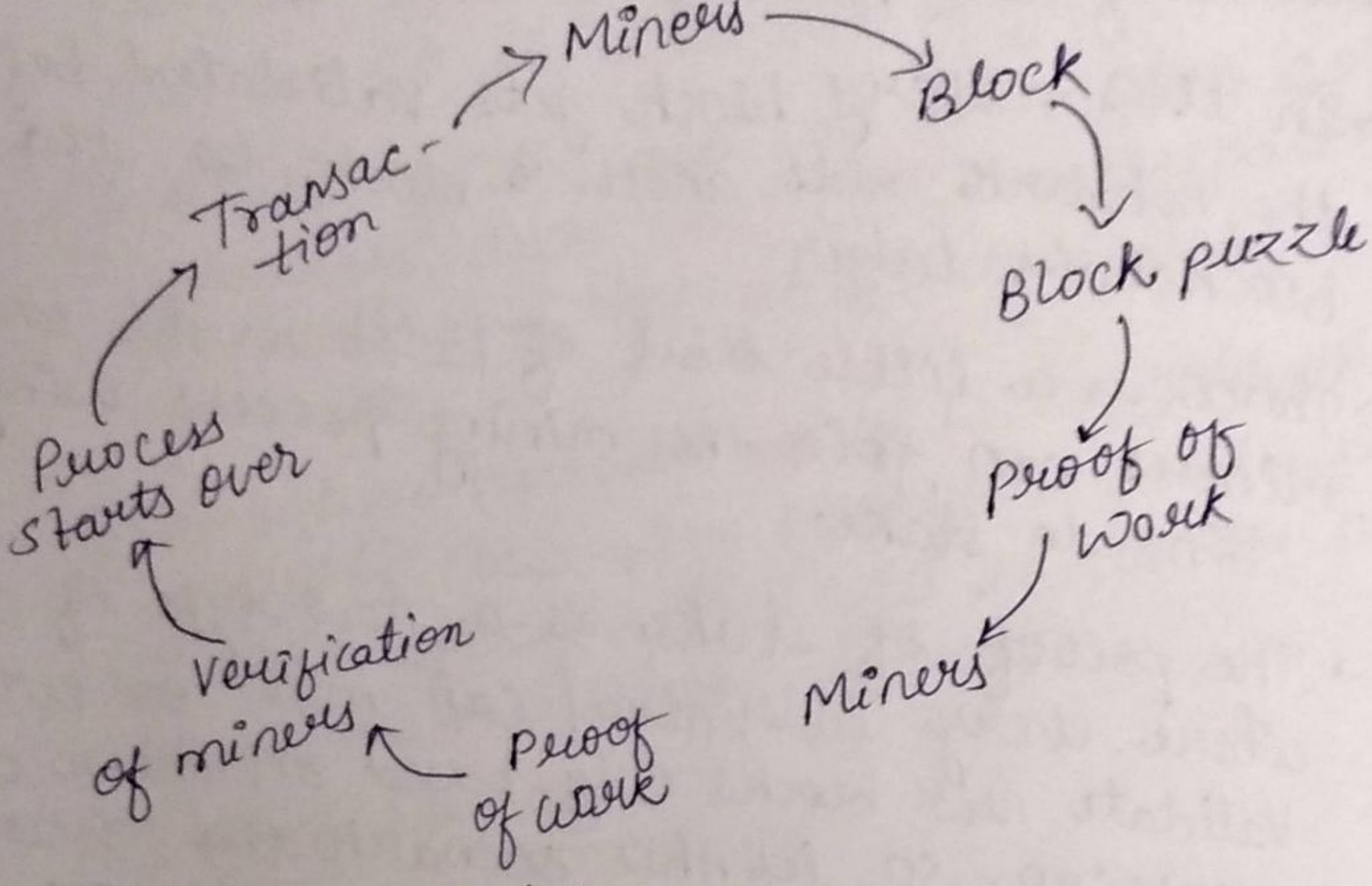
$= (4 \text{ billion}) \times (2 \times 10^{-22})$

$= 8 \times 10^{-33} = 10^{-32}$

$= 0.0000\ldots1\%$

A modest miner can create 100 million hashes per second. To traverse 4 billion hashes, takes just 40 seconds.

→ Broadcasting proof of work in network :-



→ Bitcoin Network :-

The bitcoin network is a P2P payment network that operates on a cryptographic protocol. Users send and receive bitcoins, the units of currency, by broadcasting digitally signed messages to the network using bitcoin cryptocurrency wallet s/w.

Bitcoin : bits & pieces

** Proof of Stake (PoS)

→ Proof of stake is a consensus algorithm blockchain that deals with the main drawbacks of the PoW algorithm.

→ In this, every block gets validated before the network adds another block to the blockchain ledger.

→ There is a little bit of Twist in this one. Miners can join the mining process using their coins to stake.

→ The proof of stake is a new type of concept where every individual can mine or even validate new blocks only based on their coin possession. So, in this scenario the more coins you have, the better your chances are.

keypoints!

(i) The mining capability of a particular miner depends on how many coins he/she already has.

(ii) The 51% attack is ridiculously expensive in the Proof of Stake (PoS) method.

(iii) The community-bond of the stakeholders of PoS is not that strong. So, PoS-community is more decentralized.

Pooling

→ There are other ways to participate in the staking. If the staking amount is too much high, then you can join a pool and earn profits through that.
You can do it in two ways :-

(i) First of all, you can loan your coin to another user who will participate in the pool and then share the profit with you.

(ii) Another method would be to join the pool yourself. This way everyone participating in that specific pool will divide the profit based on the stake amount.

PoS state Diagram

→ PoS : Advantages:

(i) First of all, this type of consensus algorithms doesn't require any amount of heavy hardware backup. You only need a functional computer system and a stable internet connection.

(ii) PoS consensus algorithm blockchain is much more energy efficient than proof of work.

(iii) It doesn't need too much power consumption.

(iv) It also reduces the threat of a 51% attack.

→ Pos : Issues

(i) The main drawback of the system is that full decentralization is not possible ever. This is simply bcoz only a handful of nodes get to participate in the staking on the network. Individuals with the most coins will eventually control most of the system.

(ii) Popular Cryptocurrencies Using Proof of Stake as the base of the blockchain technology.

- PIVX
- Navcoin
- Stratis

→ PoS requires people to prove the ownership of a certain amount of currency.

→ Many blockchains adopt PoW at the beginning and transform to PoS gradually.

→ PoS alternatives ~~as~~ consume less energy and reach higher transactions per second.

→ Challenge for proof-of-stake systems is to keep track of the changing stakes of the stakeholders.

→ Different versions:
random selection, age based stake selection (number of coins stake multiply by the time they have been staked, when selected, time reset to 0)...

PoS: Randomization

~~Blockch~~
— Blackcoin uses randomization to predict the next generator.
— It uses a formula that looks ~~a~~ for a true lowest hash value in combination with the size of the stake.

PoS: Coin age:-

— Peercoin favours coin age-based selection.
— In peercoin, older and larger sets of coins have a greater probability of mining the next block.
— Once a user has forged a block, their coin age is reset to zero and then they must wait at least 30 days again before they can sign another block.

→ Proof of Work Vs Proof of Stake:

Proof of Work (PoW)	Proof of Stake (PoS)
(1) The probability of mining a block is determined by how much computational work is done by miner	(1) The probability of validating a new block is determined by how large of a stake a person holds. (how many coins they possess).
(2) A reward is given to first miner to solve cryptographic puzzle of each block.	(2) The validator donot receive a block reward instead they collect network fee as their reward.
(3) To add each block to chain, miners must compete to solve difficult puzzles using their computer process power.	(3) There is no competition as block creator is chosen by an algo based on user stake.
(4) Hackers would need to have 51% of computational power to add malicious block.	(4) Hackers would need to own 51% of all cryptocurrency on network, which is practically impossible.
(5) Proof of work systems are less energy efficient and are less costly but more proven.	(5) Proof of Stake systems are much more cost and energy efficient than PoW systems but less proven.

⑥ Specialized equipment to optimize processing power.
⑦ Initial investment to buy hardware.

⑥ Standard server grade unit is more than enough.
⑦ Initial investment to buy stake and build reputation.

** Delegated Proof of Stake (DPoS) :—

Intro.

— Delegated Proof of Stake is a variation of the typical proof of stake. The system is quite robust and adds a different form of flexibility to the whole equation.

— If you want fast, efficient, decentralized consensus algorithms then Delegated Proof of Stake would be the best way to go.

— Here, instead of miners or Validators, the nodes are called delegates. By determining block production, this system can make a transaction within just one second.

→ DPoS system is maintained by an election system for choosing nodes which verify blocks. These nodes are called "witnesses" or "block producers".

Here is how DPoS consensus works:

Voting :-

→ In DPoS consensus users can either directly vote or give their voting power to another entity to vote on their behalf.

→ Selected witness are responsible for creating blocks by verifying transactions.

→ If they verify and sign all transactions in a block, they receive a reward.

→ If a witness fails to verify all transactions in the given time, block is missed.
↳ Such transactions are collected by the next witness, and such a block is called stolen.

→ Witnesses :-

- Witnesses are responsible for validating transactions and creating blocks, and are in return awarded associated fees.

- Witnesses can prevent specific transactions from being included in block but they cannot change info. of any transaction.

- Around in a DPoS blockchain with N block producers/witnesses follows a round robin order.

Delegates

- Users in DPoS systems also vote for a group of delegates who oversee blockchain governance

- They don't play a part in transaction control.

- Delegates can propose changing size of a block, once delegates propose such changes, blockchain users vote on whether to adopt them.

Block Validators:-

- Block validators in DPoS refer to full nodes who verify that blocks created by witnesses follow the consensus rules.

Advantages:-

(1) DPoS blockchains have good protection from double-spending.

(2) It is more democratic and financially inclusive due to lesser staking amount required by a user/node.

(3) DPoS provides more decentralization as more people take part in the consensus due to low entry threshold.

(4) It doesn't require lot of power to run network, which makes it more sustainable.

(5) DPoS method provides foundation for implementing interesting governance models in blockchain applications. In a sense, it forms a kind of democracy.

Disadvantages:-

(1) Effective operation and decision making of network requires delegators to be well informed and appoint honest witnesses.

② Limited no. of witnesses can lead to centralization of network.

③ DPos blockchain is susceptible to problems of weighted voting. Users with smaller ~~te~~ stake can refuse from taking part in votings after considering that their vote is insignificant.

e.g. of blockchain platform using DPoS: Lisk

* Distributed system:-

Distributed systems are built for high availability and scalability involving a group of computers or a set of distinct processes working together to accomplish a common objective.

Emails, web browsers, and many other mainstream software such as Netflix Eureka and Apache Zookeeper, all use distributed system algorithms.

Some of the challenges faced in distributed systems are:-

ⓐ clock drift
ⓑ concurrency
ⓒ Message transmission
ⓓ component failure.

* Paxos - A distributed consensus algorithms:
Paxos is an algorithm that is used to achieve consensus among a distributed set of computers that communicate via an asynchronous network.
The primary paxos mechanism works under the principle that if the majority of the nodes agree on a value, then consensus is ~~acchi~~ reached.
It has three roles:

(1) Proposer :- A proposer receives client requests called 'values' and sends these proposed values to acceptors.

(2) Acceptor :- Receives messages from proposers and learners. They view the proposed values and inform the proposer whether they accept or reject the proposed value

(3) Learner :- Listen to all the acceptor's decisions and delivers values in an ordered sequence.

→ There are two phases in the underlying PAXOS protocol.

Phase-I :

→ A proposer prepares a unique number N and gets acceptors to accept the proposed number N, i.e. get their promise to accept the values within a set timeout period.

→ If any acceptor has previously accepted a value, he or she should inform the proposer of the already accepted proposal number and value.

→ The acceptors will accept N only if it is higher than the proposal no. value they have

stored.

Phase II :- Here, the proposers check if they got the majority vote, i.e whether they can use theire proposal or whether they have to use the highest-numbered one received from among all the responses.

** Leased Proof of Stake (LPoS):

This consensus algo. blockchain was introduced to by Waves platform.

→ In leased proof of stake, the small-holders can finally get their chance of staking. They can lease their coins to the network and take the benefit from there.

* Proof of Elapsed Time:

— This algo is used mainly on permissioned blockchain network, where we'll have to get permission for accessing the network.

— These permissions networks need to decide on the mining rights on voting principles.

— Every individual on the network has to wait for an amount of time.

— PoET depends on a special CPU requirements. It's called intel s/w Guard Extension (intel SGX).

→ Practical Byzantine Fault Tolerance (PBFT):-

— PBFT mainly focuses on the state machine. It replicates the system but gets rid of the main Byzantine general problem.

— The algorithm is designed for asynchronous consensus systems and further optimized in an efficient way to deal with all the problem.

— Its goal was to solve many problems associated with already available Byzantine Fault Tolerance solutions.

→ A pBFT system can function on the condition that the maximum number of malicious nodes must not be greater than or equal to one-third of all the nodes in the system. As the number of nodes increase, the system becomes more secure.

Advantages of Pbft:-

(i) Energy efficiency: pBft can achieve distributed consensus without carrying out complex mathematical computations.

(ii) Transaction finality:
The transactions do not require multiple confirmations after they have been finalized and agreed upon.

(iii) Low reward variance: Every node in the network takes part in responding to the request by the client ~~and hence every node~~.

Drawback

→ Communication Gap:-

— The most important factor of this algorithm is the communication among the nodes. Every node on the network has to make sure that the info. they gather is solid.

— If the group of nodes increases to a great extent, the system may find it hard to keep track ~~it~~ of all the nodes and can't communicate with every single one of them.

→ Proof of capacity
→ Proof of Deposit
→ Proof of Activity
→ Proof of Burn
→ PBFT drawback 2